IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

CryptoMapAI: AI Based Tracing of Suspicious Cryptocurrency Trasnscation Across Multiple Blockchains

Arjun Kadam[1], Sudhir Dongargave[2], Akash Chindhe[3], Prof. Gunjal. H. D[4]
Department of Computer Engineering[1-4]
Vishwabharati Academy College of Engineering , Ahilyanagar, India
akashchindhe458@gmail.com , kadamarjun171@gmail.com , sudhirdongargave@gmail.com

Abstract: *The rapid adoption of cryptocurrencies has transformed the digital financial ecosystem by enabling decentralized and borderless transactions. While blockchain technology offers transparency and security, it has also become a medium for illicit activities such as money laundering, ransomware payments, cryptocurrency theft, fraud, and darknet transactions. Traditional investigation techniques face significant challenges due to the pseudonymous nature of blockchain networks and the use of privacy-enhancing mechanisms such as mixers, tumblers, and cross-chain transactions. Researchers have proposed various blockchain forensic systems, machine learning models, and graph-based analytics approaches to detect suspicious transactions and identify criminal activities. This survey paper presents a comprehensive review of recent developments in cryptocurrency fraud detection and blockchain transaction tracing. The study examines machine learning-based fraud detection systems, graph-theoretic transaction analysis, blockchain crime tracking frameworks, and security mechanisms for cryptocurrency networks. Furthermore, it highlights existing limitations and identifies research gaps that motivate the development of advanced solutions such as CryptoMapAI. The survey concludes with future research directions for AI-powered blockchain forensic systems.*

Keywords: Cryptocurrency Fraud Detection, Blockchain Forensics, Machine Learning, Transaction Analysis, Graph Analytics, Artificial Intelligence

I. INTRODUCTION

Cryptocurrencies such as Bitcoin, Ethereum, Monero, and Zcash have emerged as significant innovations in the financial sector. Their decentralized architecture eliminates the need for intermediaries and enables secure peer-to-peer transactions. Despite these advantages, the widespread adoption of cryptocurrencies has introduced serious challenges in financial security and cybercrime investigation.

The pseudonymous nature of blockchain transactions allows users to conduct financial activities without directly revealing their identities. Criminal organizations exploit this characteristic to perform money laundering, ransomware attacks, fraud schemes, darknet market transactions, and illegal fund transfers. As a result, law enforcement agencies and financial institutions require sophisticated analytical tools capable of identifying suspicious transaction patterns and tracing illicit fund movements.

Recent advances in Artificial Intelligence (AI), Machine Learning (ML), blockchain analytics, and graph theory have significantly enhanced the ability to analyze large-scale blockchain data. Researchers have proposed multiple approaches for transaction classification, anomaly detection, criminal wallet identification, and transaction flow visualization. This survey reviews these contributions and discusses their strengths, limitations, and applicability in modern cryptocurrency investigations.

DOI: 10.48175/IJARSCT-37108

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

II. LITERATURE REVIEW

A. Graph-Based Cryptocurrency Transaction Tracking

Subbotin et al. proposed a graph-theoretic approach for tracking cryptocurrency transactions by representing wallets as graph nodes and transactions as edges. Their system recursively discovers connected wallets and visualizes transaction relationships to identify potentially suspicious networks. The study demonstrated that graph analytics can effectively uncover hidden relationships among blockchain addresses and support criminal investigations. However, the approach primarily focuses on visualization and lacks intelligent classification mechanisms for automated fraud detection.

B. AI-Based Fraud Detection Systems

Machine learning has become one of the most promising approaches for detecting fraudulent cryptocurrency transactions. Several studies have employed supervised and unsupervised learning algorithms to analyze transaction behavior and identify anomalies. Random Forest, Gradient Boosting, Isolation Forest, Autoencoders, and Graph Neural Networks have shown promising performance in recognizing suspicious activities.

These approaches analyze transaction frequency, transaction value, wallet interactions, and temporal behavior patterns to distinguish legitimate transactions from fraudulent ones. However, many existing solutions rely on static datasets and often struggle to generalize to emerging fraud techniques and evolving blockchain ecosystems.

C. Criminal Transaction Pattern Analysis

Recent research on criminal transaction behavior focuses on understanding how cybercriminals transfer and conceal illicit funds. Studies examining thief wallet activities in Ethereum networks have revealed common patterns such as fund splitting, intermediate wallet usage, exchange interactions, and delayed cash-out strategies. Researchers have also investigated transaction mixing techniques such as CoinJoin and tumbling services that obscure transaction origins and destinations.

Although these studies provide valuable insights into criminal behavior, they often concentrate on specific attack scenarios and lack comprehensive frameworks capable of analyzing multiple blockchain platforms simultaneously.

D. Blockchain-Based Crime Tracking Systems

Blockchain technology itself has been proposed as a solution for tracking and recording criminal evidence. Crime tracking systems built on blockchain infrastructures offer transparency, immutability, and auditability. Such systems improve accountability and maintain tamper-proof records for forensic investigations.

However, existing blockchain-based crime tracking solutions mainly focus on evidence management rather than cryptocurrency transaction analysis. Therefore, they are insufficient for tracing complex financial crimes involving multiple blockchain networks and anonymization mechanisms.

E. Security Analysis of Cryptocurrency Networks

Security researchers have extensively studied vulnerabilities in cryptocurrency networks. Investigations into Bitcoin peer-to-peer networking have identified weaknesses such as denial-of-service attacks, Sybil attacks, and misbehavior tracking limitations. These vulnerabilities can potentially affect transaction monitoring systems and compromise network integrity.

Understanding such security challenges is essential when designing robust blockchain forensic systems capable of operating in adversarial environments.

III. COMPARATIVE ANALYSIS OF EXISTING APPROACHES

The comparison indicates that no single approach fully addresses the complex challenges of cryptocurrency fraud detection, transaction tracing, criminal identification, and cross-chain analysis. This underscores the core motivation for establishing unified, multi-layered framework systems.

APPROACH	TECHNIQUE USED	ADVANTAGES	LIMITATIONS
Graph-Based Tracking	Graph Theory, Visualization	Reveals comprehensive wallet relationships and structural topologies.	Limited intrinsic fraud classification for automated alerting.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, June 2026 Impact Factor: 8.2

Machine Learning Detection	Random Forest, Isolation Forest	Achieves high analytical and classification detection accuracy.	Requires large quantities of high-quality training datasets.
Criminal Pattern Analysis	Transaction Flow Analysis	Effectively identifies complex laundering routes and behaviors.	Exhibits limited architectural scalability on massive ledgers.
Blockchain Crime Tracking	Blockchain Records	Guarantees complete evidence transparency and data integrity.	Not inherently focused or optimized for transaction tracing.
Network Security Analysis	Security Monitoring	Successfully detects infrastructural attacks and node vulnerabilities.	Does not actively analyze transaction behavioral analytics.

IV. RESEARCH GAPS

The extensive literature review highlights several significant research gaps that current frameworks fail to address adequately:

• Limited Cross-Chain Analysis: Most existing systems focus strictly on a single blockchain network and fail to track complex cross-chain bridges and multi-platform asset transfers.

• Insufficient Real-Time Detection: Many forensic solutions are bounded to historical, static datasets rather than active, near real-time blockchain stream ingestion.

• Lack of Integrated Intelligence Sources: Current structural models rarely combine live on-chain ledgers with external threat intelligence repositories like darknet markets or flagged hacker address blacklists.

• Poor Explainability: Advanced black-box AI fraud systems provide risk weights without explaining the exact behavioral vector triggers, decreasing legal admissibility.

• Scalability Challenges: Computational overhead rises exponentially when using standard recursive graph calculations on massive modern transaction graphs.

• Identity Attribution Difficulties: Mapping alphanumeric keys back to actual real-world entities is easily disrupted by privacy coins and obfuscation mixers.

V. CRYPTOMAPAI: FUTURE DIRECTION FOR BLOCKCHAIN FORENSICS

To overcome the architectural shortcomings of existing technologies, advanced systems like the proposed CryptoMapAI incorporate multi-layered machine learning algorithms, deep graph networks, and integrated cyber threat intelligence platforms into a single unified framework.

A comprehensive blockchain forensic system should include the following structural layers:

• Multi-blockchain transaction monitoring capable of parsing transparent public ledgers alongside privacy-centric environments.

• AI-based anomaly detection utilizing ensemble methods like Random Forest (achieving up to 99% experimental accuracy) alongside unsupervised tools like Isolation Forests and Autoencoders.

• Graph clustering and transaction network visualizations utilizing structural methodologies like Markov Chain Analysis and DBSCAN.

• Integration with off-chain criminal telemetry, flagged wallet directories, and darknet intelligence networks.

• Dynamic real-time risk scoring and Explainable AI (XAI) mechanisms to render model evidence transparent for legal, investigative, and court presentation.

DOI: 10.48175/IJARSCT-37108

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, June 2026
Impact Factor: 8.2

VI. CONCLUSION

The increasing use of cryptocurrencies has created new opportunities for innovation while simultaneously introducing serious security and regulatory challenges. Researchers have proposed numerous approaches for transaction tracking, fraud detection, criminal behavior analysis, and blockchain-based evidence management. Graph analytics, machine learning, blockchain forensics, and network security mechanisms have each contributed valuable insights toward combating cryptocurrency crime.

However, existing solutions remain fragmented and face limitations related to scalability, real-time analysis, explainability, and cross-chain transaction tracing. This survey identifies these shortcomings and highlights the need for integrated AI-driven forensic platforms. Future systems such as CryptoMapAI (leveraging advanced components like the ChainGuard-V1 Engine) bridge these gaps by combining machine learning, graph-based analytics, and blockchain intelligence to provide more accurate, scalable, and efficient cryptocurrency fraud detection capabilities.

REFERENCES

[1] D. A. Subbotin, M. A. Antropova, and P. V. Sukharev, “Tracking Transactions in Crypto Currencies Using the Graph Theory,” IEEE, 2020.
[2] S. Rattanabunno and W. Werapun, “Decrypting Criminal Transaction Patterns in Cryptocurrency,” IEEE, 2023.
[3] H. S. Kabiru, A. J. Jika, and R. Mishra, “Company Crime Tracking System Using Blockchain,” IEEE, 2024.
[4] W. Fan et al., “Security Analyses of Misbehavior Tracking in Bitcoin Network,” IEEE ICBC, 2021.
[5] B. A. Ramadhan and B. M. Iqbal, “User Experience Evaluation on the Cryptocurrency Website by Trust Aspect,” IEEE, 2018.
[6] S. Pawar, R. Tokle, A. Walunjkar, and K. Shingade, “CryptoMapAI: A Machine Learning-Based System for Fraud Detection in Cryptocurrency Transactions using ChainGuard-V1 Engine,” 2025.
[7] S. Yerram et al., "AI-based cryptocurrency monitoring systems," Journal of Digital Finance, vol. 12, no. 3, pp. 245-260, 2020.
[8] T. Gao, "Machine learning applications for Ethereum fraud detection," Blockchain Technology Review, vol. 5, no. 1, pp. 78-92, 2023.
[9] A. Rajput and M. Yousaf, "Cross-chain transaction malleability and analysis," Cryptocurrency Research, vol. 8, no. 2, pp. 145-160, 2021.
[10] M. Bartoletti et al., "Multi-label classification for scam detection in blockchain networks," ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1-25, 2021.
[11] P. Farg, M. Shahbazi, and Y. Byun, "Graph Neural Networks for transaction network analysis," IEEE Access, vol. 10, pp. 23456-23470, 2022.